Freedom Defended

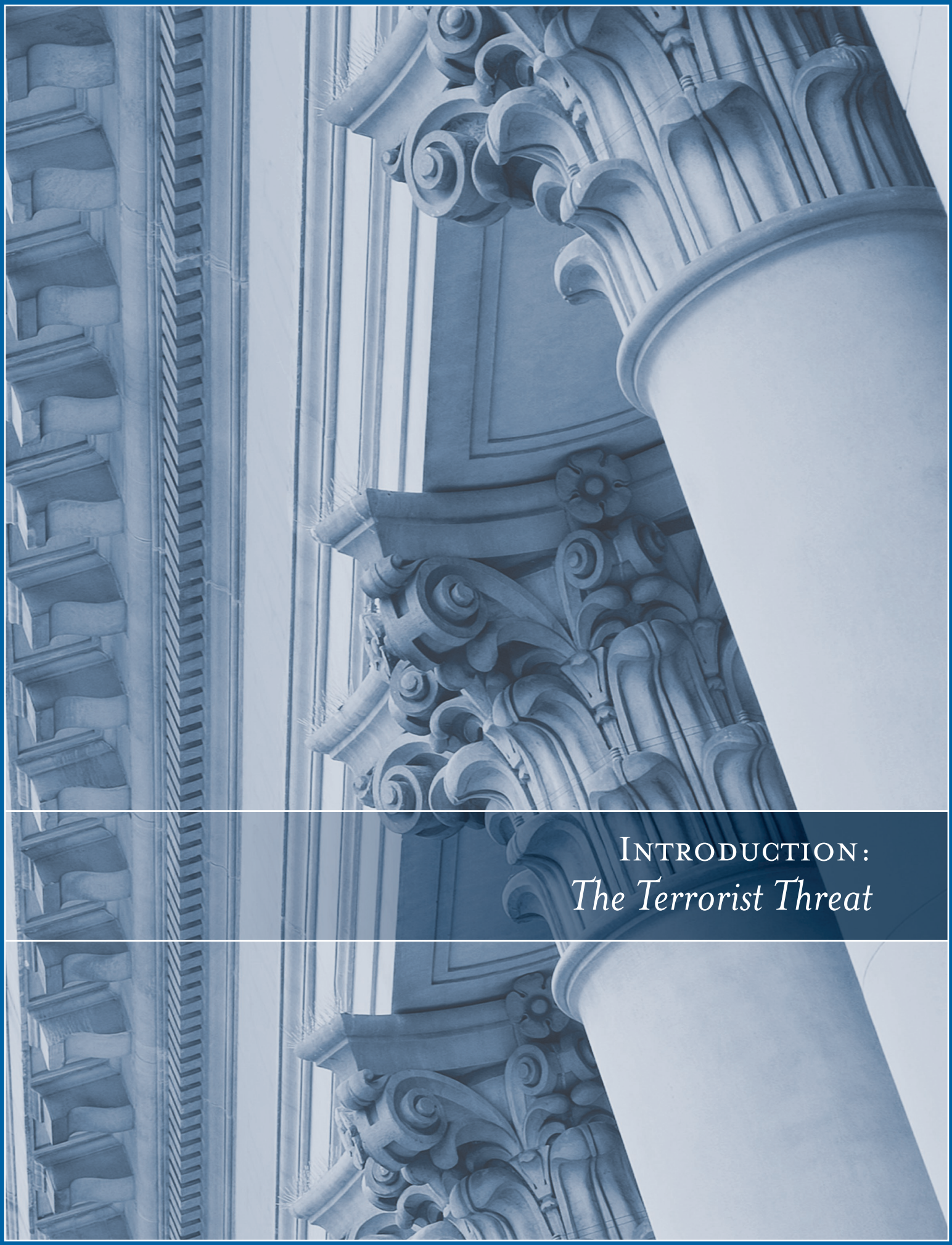
Implementing America's Strategy for Homeland Security

Select Committee on
Homeland Security
Christopher Cox, Chairman

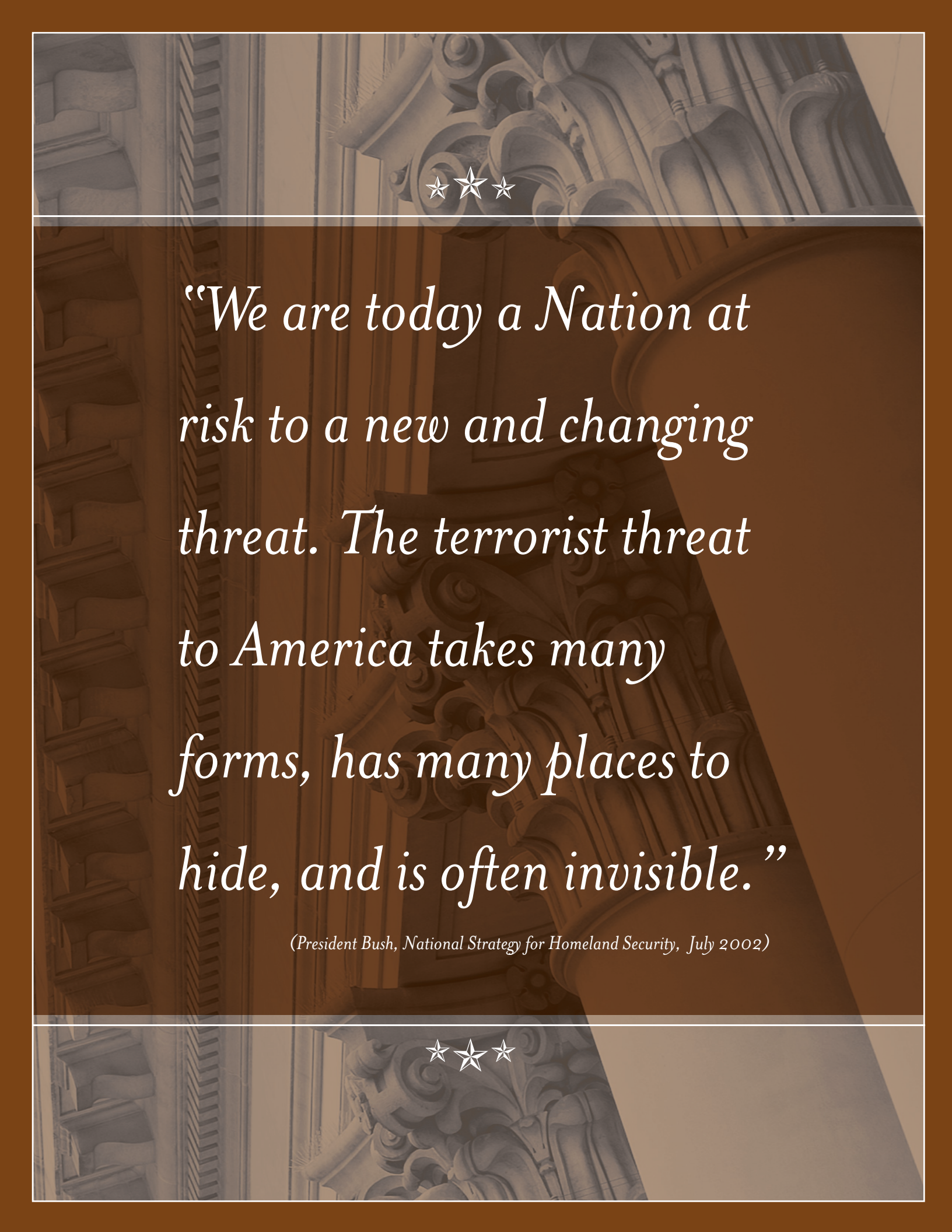
Contents

"September the 11th brought out the best in America, and the best in this Congress. And I join the American people in applauding your unity and resolve. Now Americans deserve to have this same spirit directed toward addressing problems here at home. I'm a proud member of my party—yet as we act to win the war, protect our people, and create jobs in America, we must act, first and foremost, not as Republicans, not as Democrats, but as Americans."

(From the President's State of the Union Address, the United States Capitol, Washington, D.C., January 29, 2002)



Introduction: *The Terrorist Threat*



"We are today a Nation at risk to a new and changing threat. The terrorist threat to America takes many forms, has many places to hide, and is often invisible."

(President Bush, National Strategy for Homeland Security, July 2002)

Introduction

The catastrophic terrorist attacks of September 11, 2001, challenged America to defend its national territory and its way of life in unprecedented ways. Terrorists had exploited vulnerabilities of our open society to attack icons of America's public and private sectors and to destroy human life that we consider sacred. State, local, and private entities emerged as the new stakeholders in U.S. homeland security.

The President and Congress have responded boldly to that challenge. We have rallied both the government and the American people to use every available resource to counter the terrorist threat. Much has been done, and more is being done every day. This is a long-term struggle in which America will prevail.

The challenge ahead is to transform costly short-term reactions into a cost effective, long-term strategy.

Under the leadership of President Bush and the Congress, America has:

- Actively pursued terrorists abroad, destroying the al Qaeda infrastructure in Afghanistan and killing or arresting key al Qaeda leaders in other countries. The President has sent the message that this bold pursuit will continue as long as the terrorist threat persists.
- Established the Department of Homeland Security to play a central role coordinating activities to prevent terrorism, protect our infrastructure against it, and improve our response if an attack should occur.
- Strengthened our intelligence capabilities at home and abroad, creating a global analytic fusion center for intelligence on the terrorist threat to America within the Department of Homeland Security (DHS).
- Passed laws to promote cooperation between intelligence and law enforcement officers in tracking down terrorists and their supply networks.
- Built closer counterterrorism relations with nations around the world at the military, political, and intelligence levels. These relationships, critical in the war against terrorism, have never been stronger. We must be certain that they endure.

Congress established the Department of Homeland Security to focus and strengthen the counterterrorist capabilities of 22 separate federal agencies that are now incorporated into the Department. Two key DHS elements, the Directorate of Information Analysis and Infrastructure Protection and the Directorate of Science and Technology, enhance the counterterrorism capabilities of those legacy agencies. DHS is charged with developing and driving a comprehensive homeland security strategy for the entire federal government.

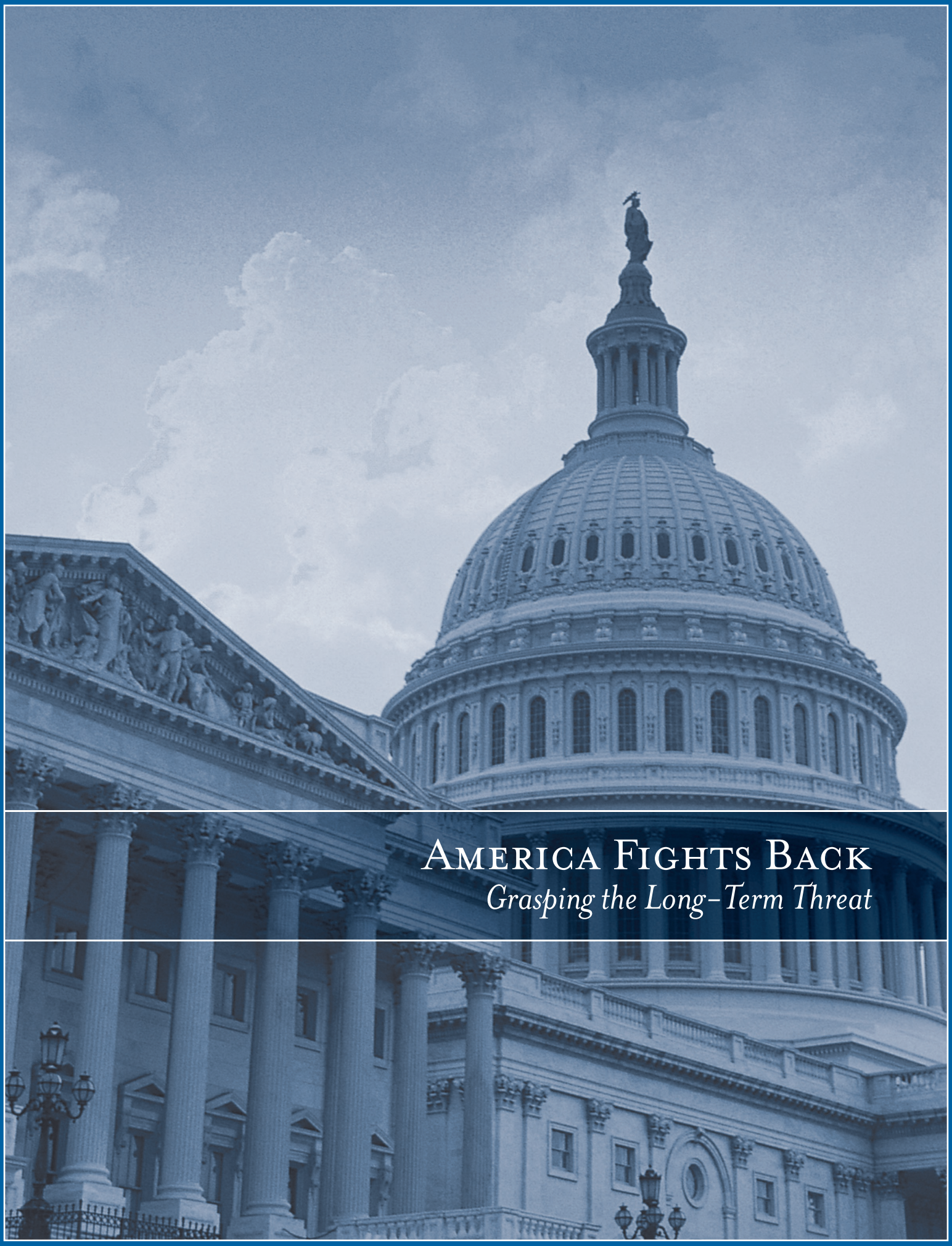
In the Congress, Speaker Dennis Hastert established the House Select Committee on Homeland Security to focus widely-dispersed Congressional oversight over the new Department, and a new Subcommittee for Homeland Security in the Committee on Appropriations to appropriate funds to the Department.

Terrorism is an enduring threat and homeland security is a permanent mission to protect America against the enemies of freedom. In the year ahead, Congress will be challenged to focus jurisdiction of homeland security on its critical counterterrorism mission to prevent, protect, and respond.

Christopher Cox, *Chairman, Select Committee on Homeland Security*

"Terrorists seek to infiltrate our society, scope out targets, and wage war in our streets and cities."

(Secretary Ridge, "Remarks Marking the One-Year Anniversary of the Creation of the Department of Homeland Security," February 23, 2004)



America Fights Back

Grasping the Long-Term Threat

"Our society presents an almost infinite array of potential targets that can be attacked through a variety of methods."

(President Bush, National Strategy for Homeland Security, July 2002)

On September 11th, terrorists transformed passenger airlines into missiles, striking first at our nation's financial and military centers but intending to reduce the American people's confidence in their commitment to freedom at home and abroad. They want us to be paralyzed by fear and to respond in ways that will weaken our economy, erode our freedoms, and force our retreat from global leadership.

In this, the terrorists failed. America, under President Bush's leadership, has preserved its freedoms and is more committed than ever to defending our way of life. Since 9/11, we have reduced our vulnerabilities at home and aggressively pursued terrorists abroad while growing our economy and preserving our freedoms.

The terrorist threat to America is dynamic, constantly adapting to our countermeasures. We must be vigilant in adjusting and strengthening our security measures, recognizing that this is a long-term struggle in which we must stay ahead of the enemy.

Al Qaeda is a network of individuals, cells, and front organizations spanning the world and threatening freedom everywhere. Driven by a fanatical political ideology, al Qaeda still has the will and the capability to strike America and her interests anywhere in the world, including within our borders. Al Qaeda supporters have been arrested in Buffalo and Albany, New York; Portland, Oregon; as well as in the United Kingdom, Germany, Spain, Italy, Pakistan, Indonesia and other places around the world.

Al Qaeda terrorists are seeking chemical, biological, radiological, and nuclear materials to attack America, according to the Central Intelligence Agency (CIA). The destructive potential of these weapons appeals to terrorists who want to inflict massive casualties. In the future, if we do not stop them they will use these horrific weapons against us. We have no option but to engage and defeat them now wherever they are.

The Bush Offensive

President Bush knows that America has been forced into a war with terrorists, and that we are better off fighting them abroad than at home. America is now attacking the terrorists where they live, in Afghanistan, Iraq, Pakistan, the Philippines, Indonesia, and elsewhere around the world. Within weeks of September 11th, we had taken the battle to the enemy in Operation Enduring Freedom in Afghanistan, destroying al Qaeda's infrastructure and removing the Taliban regime that protected it. Here, where al Qaeda colluded with the Taliban regime to foster terrorism against America, we not only pursed counterterrorist objectives, but also liberated the Afghani people from a brutal reign of terror under the Taliban.

> *"The best defense against terrorism is a strong offensive against terrorists."*
>
> *(President Bush, "Radio Address of the President to the Nation," October 13, 2001)*

In March 2003, together with a 48-country coalition, the United States embarked on Operation Iraqi Freedom. We removed one of the world's leading anti-American dictatorships, and simultaneously liberated 25 million Iraqis at a high cost to American blood and treasure. This historic action has opened the way for democracy in Iraq, for a better life for all Iraqis and, most importantly, for long-term stability in the Middle East.

Today, America along with NATO allies and coalition partners from around the world continues operations against al Qaeda, the Taliban, and Iraqi insurgents. In Afganistan, the newly revived Afghan National Army is assisting coalition forces to hunt down remnants of the Taliban regime and the al Qaeda forces they harbored. The transition of Iraqi sovereignty on 28 June offered new hope that this strategic country will return soon to the community of responsive nations.

The United States is leading the world in providing humanitarian assistance and reconstruction to Afghanistan and Iraq so they will never again become havens for terrorists. America is assisting in the building of schools and hospitals, the repair of roads, reconstruction of bridges, and the rehabilitation of water wells, canals, dams, and water systems. Most important, the United States is building confidence among these peoples that they can govern themselves in democratic societies.

On 28 June 2004, two days prior to the announced transition date, America fulfilled its

promise of handing over the Iraqi government to its own people. To assist Iraq in the democratization process, the United States is winning the support of the international community. A multinational force was unanimously approved by a United Nations Security Council resolution. NATO also pledged to provide training for the new Iraqi government's security forces.

Fostering International Collaboration

The United States continues to coordinate with friends and allies abroad to track, capture, or kill terrorists wherever they hide. This offensive strategy is a vital part of America's comprehensive strategy to protect the homeland.

1. The U.S.-led global partnership against terrorism is reducing the threat of catastrophic terrorism within the United States and abroad. Working together with key allies such as the United Kingdom, Pakistan, and Australia, the United States is successfully disrupting terrorist plans and operations.

2. Leader by leader and member by member, America and its allies are hunting down al Qaeda in dozens of countries around the world. Of the senior al Qaeda leaders, operational managers, and key facilitators identified and tracked by the U.S. government over the past three years, nearly two-thirds have been killed or taken into custody, according to the CIA. The deaths or detention of senior al Qaeda leaders, including Khalid Sheik Muhammad, the mastermind of 9-11, and Muhammad Atef, Usama Bin Ladin's second-in-command until his killing in late 2001, exemplify this record of success abroad.

America's Defense

The first lesson of September 11th was that we were not prepared at home to prevent a catastrophic terrorist attack. President Bush moved quicky to begin closing this gap.

The President outlined three strategic objectives in his *National Strategy for Homeland Security* (July 2002):

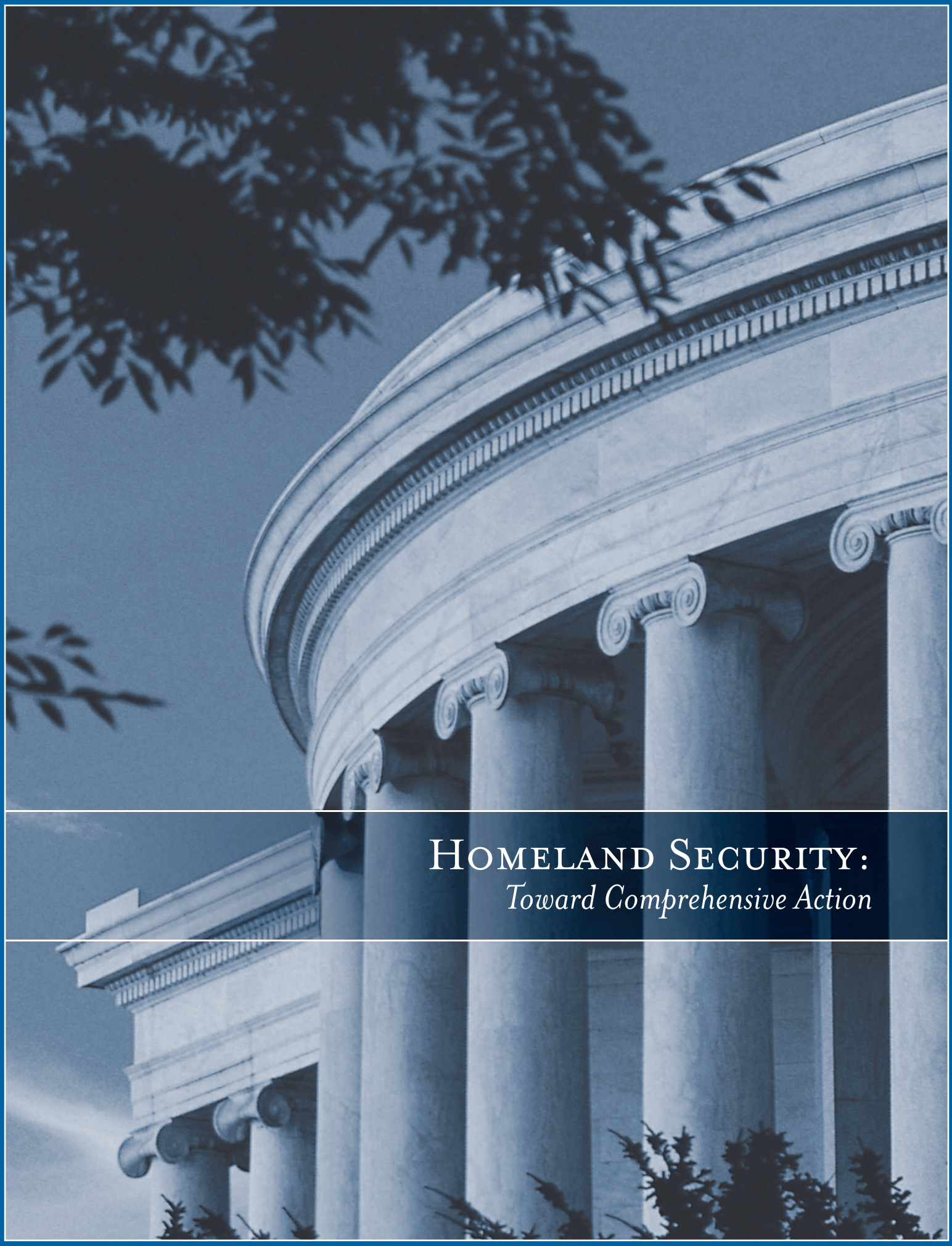
- To prevent terrorist attacks within the United States
- To reduce America's vulnerability to terrorism
- To minimize the damage and recover from attacks that, despite our increased vigilance, may occur

The Bush administration, with a strengthened hand from Congress, has done more in the past two years to enhance the security of our borders, ports, and critical infrastructure than at any time since World War II. It has invested more to improve our intelligence capabilities than any administration in a generation.

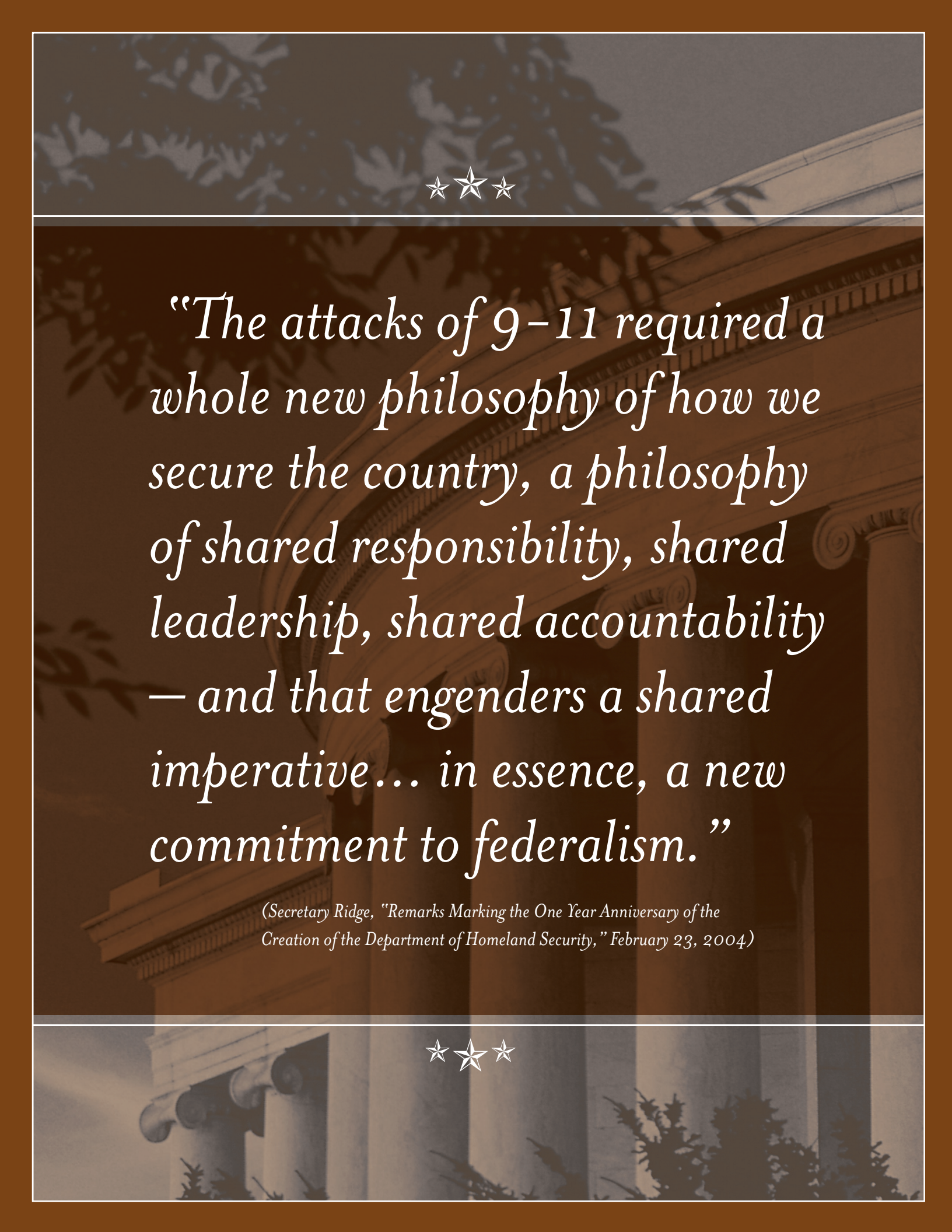
It has made significant progress in integrating our foreign and domestic threat analysis, and in building collaboration between intelligence and law enforcement at every level of government. Through the USA PATRIOT Act, Congress and the President took practical action to promote the free flow of critical information between the law enforcement and intelligence community to "tear down the wall."

Yet the President and the Congressional leadership are clear that we must do more:

- To develop and implement a clear strategy for homeland security that will direct our money, resources, and energy toward the right priorities to make America safer.
- To reform our intelligence agencies to make them more responsive to the threat to the homeland.
- To strengthen the Department of Homeland Security (DHS) as the key driver of the President's strategy for homeland security.
- To boost DHS as the principal federal interlocutor with state, local, and corporate entities with regard to terrorism risk assessment and infrastructure protection.
- To ensure Congressional oversight over DHS that is comprehensive, focused, and persistent. As the 9/11 commission has observed, a permanent House Committee on Homeland Security would be best positioned to meet this need.



Homeland Security:
Toward Comprehensive Action



"The attacks of 9-11 required a whole new philosophy of how we secure the country, a philosophy of shared responsibility, shared leadership, shared accountability — and that engenders a shared imperative… in essence, a new commitment to federalism."

(Secretary Ridge, "Remarks Marking the One Year Anniversary of the Creation of the Department of Homeland Security," February 23, 2004)

The President Seizes the Initiative

Nine days after the terrorist attacks of September 11th, President Bush created a new White House Office of Homeland Security (Executive Order 13228) to coordinate the Administration's homeland security program. We could not defeat terrorism, he said, without major restructuring of the federal government. He named Pennsylvania's Governor Tom Ridge, a widely respected leader among state and local officials, to head the new office.

In mid-2002, President Bush sent a proposal to Congress to create a new cabinet-level department to focus the efforts of its twenty-two incorporated agencies against the terrorist threat, and to serve as the focal point of the broader homeland security mission for the whole federal government. Congress passed The Homeland Security Act and the President signed it in November 2002 (Public Law 107-296). The Department of Homeland Security, the largest federal merger since the Department of Defense was created in 1947, stood up on March 1, 2003.

DHS represents a creative consolidation of 22 domestic agencies, 180,000 employees, and $36 billion in legacy budgets. The Department has two new Directorates

The Department of Homeland Security represents a creative consolidation of 22 domestic agencies, 180,000 employees, and $36 billion in legacy budgets.

– Information Analysis and Infrastructure Protection (IAIP) and Science and Technology (S&T). IAIP analyzes terrorist threat-related intelligence, assesses infrastructure vulnerabilities, conducts risk assessments combining vulnerabilities and threat, and promotes sharing of relevant information with state, local and corporate entities. S&T applies state-of-the-art technologies to the development of terrorism countermeasures and fosters homeland security-related research and development. They are at the forefront of the Department's efforts to achieve its core mission: to make America safer.

The development of counterterrorism capabilities is a matter of urgency for the Department, but organized integration of DHS will take time measured in years. Nineteen financial management systems are being streamlined to reduce the number of financial centers to ten and to enable the Department to

access financial data, conduct department-wide financial analyses, and make sound financial decisions. The Department is consolidating thirteen separate contracting offices from legacy organizations to draw together a procurement program comprised of eight component organizations.

First Responders Rise to the Challenge

On September 11th, Americans were stunned to discover that the enemy was in our midst.

Firefighters, police officers, emergency medical professionals, and public works employees were the first to respond to the terrorist attacks, and it was their skill, agility, and courage that contained the national crisis. They were – and are – our first line of defense against terrorism.

It quickly became clear, however, that on September 11th human courage far exceeded the material resources, the interoperable communications systems, the shared intelligence, and both the interagency and inter-jurisdictional collaboration essential to defeat terrorism on our own soil. Government did not work and it needed to be fixed.

As we move ahead from bold reaction to intelligent strategy, it must be a top priority for us to provide our first responders with the threat-based information and the training, equipment, and other resources they need to do their jobs effectively. We must determine how best to allocate federal, state, local, and corporate resources efficiently against a multifaceted threat. And we must continuously encourage and reward interagency and inter-jurisdictional collaboration.

Chairman Cox (far right) speaking with members of the National Organization of Black Law Enforcement Executives during meeting with law enforcement community regarding the First Responder bill

Congress Takes Action

The terrorist threat, by all expert accounts, will endure long into the future. It is not a passing phenomenon. And DHS is here to stay. It is imperative, therefore, that we establish effective Congressional oversight for the long term.

Speaker Dennis Hastert recognized that with the establishment of a new department to deal with an enduring threat, a new committee was needed to help focus some 88 committees and subcommittees with jurisdiction over homeland security. Congress in January 2003 established the House Select Committee on Homeland Security to oversee DHS and to collaborate with other committees of jurisdiction to enhance their oversight.

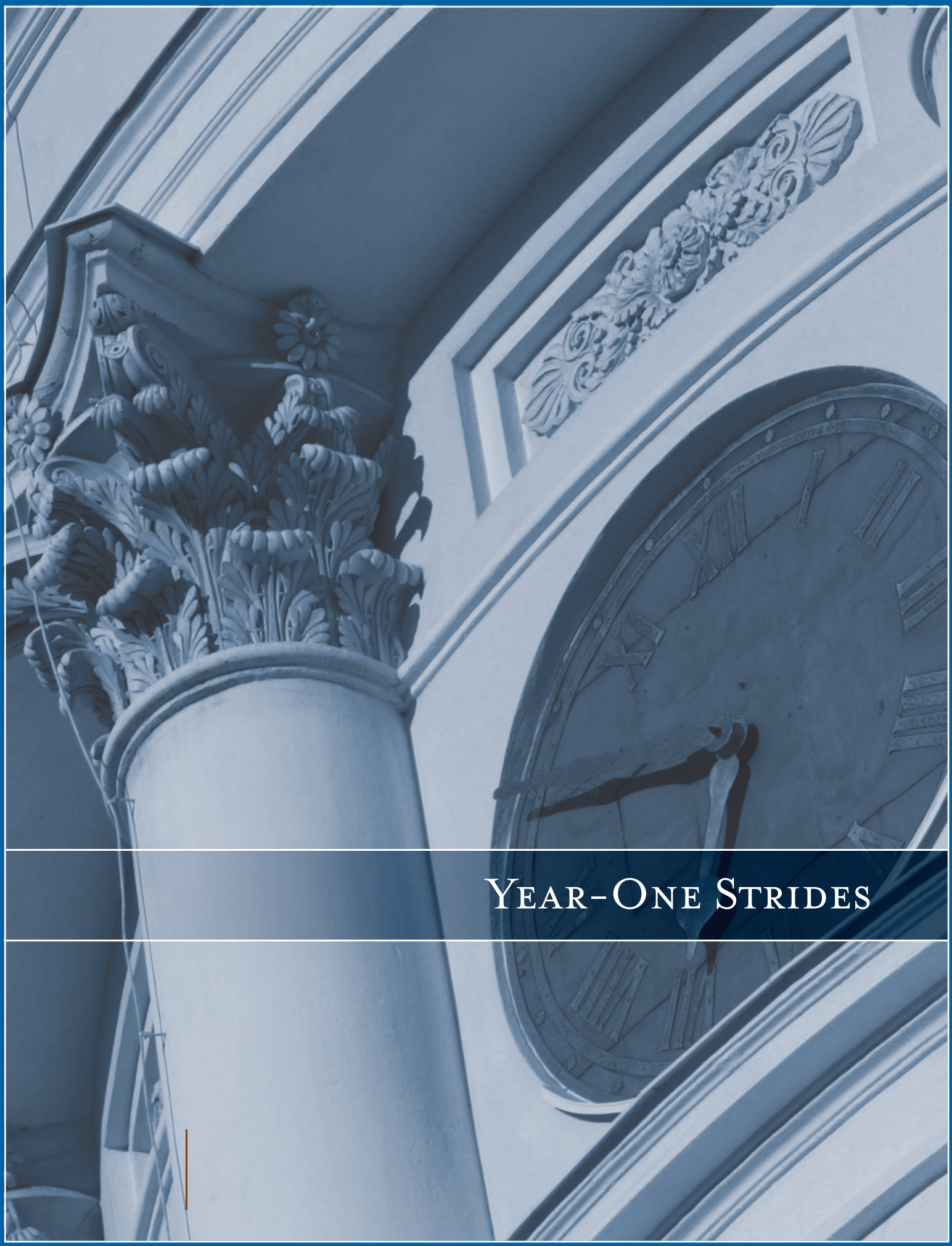
The Select Committee, working with other committees of jurisdiction, has exercised responsible oversight to improve DHS's information sharing and analysis capabilities

and to focus and discipline federal spending for first responders. It has encouraged the Department in its effort to consolidate 22 agencies. It has introduced legislation to create "one-stop shopping for grants," which will become increasingly important as the homeland security budget grows over the next several years. The Fiscal Year 2004 budget for DHS was $37.2 billion. The Select Committee has launched the process leading to the Department's first authorization bill.

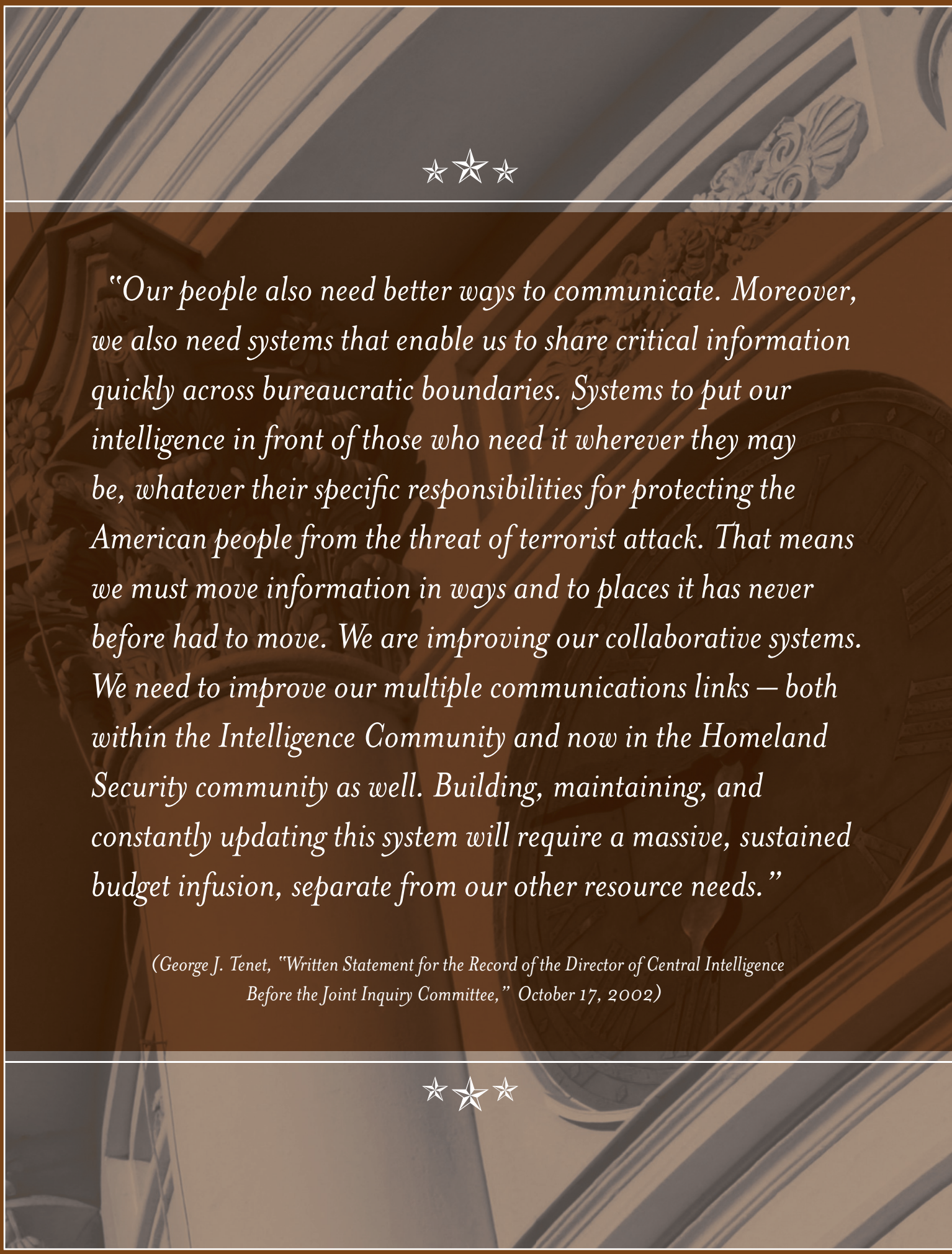
Chairman Christopher Cox (L) with Jim Turner of Texas (R) Ranking Member

"And I think we have some obligation to organize the Congress in parallel with organizing the executive branch. And I know that's very risky even for those of us who are not here but used to be to come back up here and say we actually have to look at ourselves as well as cheerfully look down the street at the executive branch. But in the case of homeland security, it is going to someday be literally life and death. And I think we'd all want to be able to look back and say to our children and our grandchildren we did the right [thing] now, not we did the easy thing."

(Former Speaker of the House Newt Gingrich, Hearing held on "Perspectives on House Reform: Former House Leaders," September 9, 2003.)



Year-One Strides



"Our people also need better ways to communicate. Moreover, we also need systems that enable us to share critical information quickly across bureaucratic boundaries. Systems to put our intelligence in front of those who need it wherever they may be, whatever their specific responsibilities for protecting the American people from the threat of terrorist attack. That means we must move information in ways and to places it has never before had to move. We are improving our collaborative systems. We need to improve our multiple communications links — both within the Intelligence Community and now in the Homeland Security community as well. Building, maintaining, and constantly updating this system will require a massive, sustained budget infusion, separate from our other resource needs."

(George J. Tenet, "Written Statement for the Record of the Director of Central Intelligence Before the Joint Inquiry Committee," October 17, 2002)

Although much remains to be accomplished, the American people should be proud of what the Department has achieved in such a short time and of the strategic direction it is now taking. There is good news across the full range of DHS's capabilities:

Sharing Information

The ability to share relevant terrorist-related information is the single most important lesson from the September 11th attacks. The Department is working diligently with all public and private sector entities – including the law enforcement and intelligence communities – to remedy this failure.

The Department

The Information Analysis and Infrastructure Protection Directorate (IAIP) was established under the Homeland Security Act to produce comprehensive analysis of threat and vulnerability-related data from all sources, public and private. IAIP assesses key vulnerabilities and maps terrorist threats against current and future vulnerabilities. It is also responsible for issuing timely warnings and taking appropriate preventive and protective action. The Homeland Security Operations Center (HSOC) provides round-the-clock operations to collect and fuse law enforcement and intelligence community information on a daily basis to help deter, detect, and prevent terrorist incidents. While this new, significant capability is continually improving, the Committee must provide strong oversight to make certain it maintains its information sharing capabilities.

Chairman Christopher Cox (R) and Secretary Tom Ridge (L), Department of Homeland Security

The **Office of Information Analysis (IA)** is developing standardized risk assessment and

Select Committee on Homeland Security — Accomplishments Timeline

★★ January 7, 2003 ★★

Congress creates the House Select Committee on Homeland Security with legislative and oversight responsibility for the Department of Homeland Security.

threat analysis to promote threat mitigation measures. IA is comprised of two principal divisions:

Risk Assessment Division (RAD)

- Charged with analyzing all incoming threats to the homeland and assessing their credibility in terms of specificity of target location, timing, and method of attack
- Provides the Office of Infrastructure Protection with assessments on terrorist capabilities, tactics, methods and training, and provides information on protective measures.

Information and Warnings Division (IWD)

- Acts as a gatekeeper for all information flowing to and from the IA
- Ensures that relevant and critical information is provided to offices within DHS and partners outside the Department, by coordinating information received by the HSOC and disseminating that information throughout the Department, to federal, state and local government agencies, and private sector partners
- Responsible for developing information sharing and intelligence requirements for internal and external partners so that necessary information reaches IA

Both divisions are building up their analytic capabilities, and the Committee must continue to provide strong oversight to ensure IA becomes a robust intelligence component for DHS.

Since its creation, IAIP has integrated five small legacy entities, including

- Critical Infrastructure Assurance Office,
- National Communications System,
- Federal Computer Incident Response Center,
- National Infrastructure Protection Center,
- And the Office of Energy Assurance.

By the spring of 2004, IAIP had disseminated over 1,000 bulletins and advisories products to its extensive customer base, containing assessment information critical to enabling homeland security.

Markup on H.R. 1416, Homeland Security Technical Corrections Act of 2003, is ordered favorably reported to the House.

The **Memorandum of Understanding (MOU)** on Information Sharing signed on March 4, 2003, by the Secretary of Homeland Security, the Attorney General, and the Director of Central Intelligence, requires all federal law enforcement, intelligence, and homeland security agencies to share terrorist-related information on an unprecedented scale. The MOU is, therefore, a practical means of advancing a critically important cultural shift among federal intelligence agencies.

Terrorist Threat Integration Center (TTIC)

- A multi-agency partnership under the Director of Central Intelligence (DCI) with DHS as a charter partner
- Incorporates for the first time all terrorist-related information, foreign and domestic, available to the U.S. Government for systematic analysis and dissemination.
- Has a critical fusion mission, which will take some time and rigorous Congressional oversight to achieve.

Full Committee hearing is held, "How is America Safer? A Progress Report on the Department of Homeland Security." Tom Ridge, Secretary of Homeland Security, gives testimony.

Terrorist Screening Center (TSC)

- Stood up on 1 December 2003 as a multi-agency partnership led by the FBI in which the Department is a participant
- Is building the capability to become a one-stop virtual shop for terrorist watch-list indications, to address one of the most serious coordination problems surfaced in the September 11th investigations.
- Will eventually access information from the watch lists of several agencies. Prior to September 11th, federal agencies maintained between 12 and 27 separate watch lists, the contents of which were not accessible across agency lines and were not comprehensively analyzed.

TSC will operate under procedures that ensure compliance with the Constitution and applicable privacy assurance laws. Any erroneous or outdated information will be corrected or deleted promptly.

The Homeland Security Committee must provide rigorous oversight to ensure that watchlists are integrated as quickly as possible and that the privacy and civil rights of all U.S. citizens are protected.

Homeland Security Information Network (HSIN)

- When fully operational, HSIN will provide a nation-wide, real-time, secure communication network for DHS, other federal agencies, state and local officials, and private sector partners using the Joint Regional Information Exchange System (JRIES). HSIN will significantly strengthen the flow of real-time threat information to state, local, and private sector partners
- HSIN is currently being deployed across the United States and was used by homeland security officials, state and local leadership, and first responders during the G-8 Summit at Sea Island, Georgia. The system will also be implemented for other upcoming National Security Special Events to strengthen the exchange of information.

Committee Recommendations

- The Secretary of Homeland Security should be made a member of all interagency boards that establish foreign intelligence collection

Full Committee hearing is held on "America's Response to Terrorism: How is the Department of Homeland Security Improving Our Capabilities?" Michael Brown, Under Secretary of Homeland Security for Emergency Preparedness and Response, gives testimony.

Chairman Christopher Cox with Vice Chairwoman Jennifer Dunn, WA, Chairman Jim Gibbons, NV, Subcommittee on Intelligence and Counterterrorism (far left), and Chairman Dave Camp, MI, Subcommittee on Infrastructure and Border Security (second from right)

requirements and priorities for estimative analysis, as well as any such boards that may be created in the future.

- A new Homeland Security Information Requirements Board should be created, with the Secretary of Homeland Security as chair of the Board and the Department's Chief Privacy Officer as a member.
- The Department must improve the secure communications and information technology infrastructure to provide for increased speed and flexibility of information sharing. The Department must also receive from the intelligence community immediate and automatic access to information related to threats of terrorist attacks.
- The Committee believes that the Department must be as precise as possible when giving threat warnings under the Homeland Security Advisory System (HSAS). The Committee encourages the Secretary to continue to improve the HSAS by making it more responsive to specific threats to regions and critical infrastructure sectors.

Committee Delegation tours the North American Aerospace Defense Command and U.S. Northern Command in Colorado and the Port of Long Beach and San Onofre Nuclear Power Plant in California.

"Facilitating the legitimate travel and business of [the 500 million people who cross the borders] is as critical to our way of life as is preventing would-be terrorist and terrorist materials from entering the country."

(Chairman Cox, Hearing held on "Assessment of Department of Homeland Security Initiatives to Secure America's Borders," June 25, 2003)

* The Department must ensure that the federal government's finished analytic products and conclusions are communicated to state, local and private sector officials in a coordinated way that prevents confusion, mixed signals, and potentially dangerous operational conflicts.

The Committee also strongly encourages the Department of Homeland Security and the Department of Justice to enter into a Memorandum of Understanding outlining how terrorist-related threat advisories, warnings, and advice will be disseminated.

Securing Borders and Ports

The Department

Border protection is a top priority for the Department. America shares 5,525 miles of border with Canada and 1,989 miles with Mexico. More than 500 million people and $1.35 trillion in trade cross these borders into the United States each year.

In enacting the Homeland Security Act, Congress recognized that maintaining border security functions across multiple federal agencies was at best a misuse of resources and at worst a gap in America's border security system. Bringing essential border security functions together within DHS, and coordinating their efforts within the Border and Transportation Security Directorate (BTS), has improved service and tightened security.

First full Committee hearing is held on "Assessment of the Department of Homeland Security Initiatives to Secure America's Borders." Asa Hutchinson, Under Secretary of Homeland Security for Border and Transportation Security, gives testimony.

DHS has been able to capitalize on the combined resources of the legacy agencies to strengthen border security and advance key initiatives.

One major change administered by the Department was the reorganization of the border inspection services into one unified force within U.S. **Customs and Border Protection (CBP)**:

- CBP Officers provide travelers and the trade community with "one face at the border" at U.S. ports of entry.
- Integrating the work of approximately 18,000 inspectors, CBP is easing the process for travelers while maximizing the ability to identify and address potential risks at the border.
- The Committee will continue to provide oversight of CBP to make certain it is focused on the homeland security mission.

Since the terrorist attacks of September 11th, thousands of additional law enforcement officers have been hired to protect our borders and ports. Beyond staffing, DHS is employing technology to aid in monitoring the borders. This technology includes underground sensors, vehicle barriers, and cameras. DHS is currently testing and deploying unmanned aerial vehicles

Markup on H.R. 2112, Project BioShield Act of 2003, is ordered favorably reported to the House.

to be used on the U.S. land border potentially allowing officers to better monitor remote border locations.

Another major initiative is the **United States Visitor and Immigrant Status Indicator Technology (US VISIT)** Program, which has been implemented ahead of schedule.

- Since January 2004, this program has been in place at U.S. international airports and seaports
- US VISIT will be expanded during the next two years to fulfill the Congressional mandate for recording the entry and exit records of all visa holders using biometric identifiers.
- From January to September 2004, over 8.1 million foreign visitors were processed by US VISIT, stopping over 1,000 individuals at U.S. ports of entry with prior or suspected criminal or immigration violations.
- As US VISIT builds its border screening capability, the Committee must ensure that it becomes an integrated border security system.

One of the most important means of improving border security is by pushing out our borders – screening passenger and cargo information prior to arrival and conducting inspections before high-risk individuals and containers reach our borders. DHS has several initiatives underway to implement this policy, including:

Container Security Initiative (CSI)

- Has been successfully expanding to extend the security perimeter to overseas ports shipping cargo to the United States
- Through CSI, CBP inspectors stationed overseas identify, target, and search high risk U.S. bound cargo at foreign ports of loading
- Since its January 2002 announcement, CSI has become operational at 24 of the world's major seaports in Europe, Asia, Africa, and North America

Customs-Trade Partnership Against Terrorism (C-TPAT)

- Is expanding and standardizing security measures worldwide to secure cargo from its point of origin, through the supply chain, to its final destination

(L-R) Chairman Cox, Deputy Director of Central Intelligence John McLaughlin, Committee Staff Director John Gannon, Director of Central Intelligence George Tenet, Ranking Member Turner, and Former Director of Central Intelligence William Webster

- Is a partnership between the federal government and the trade community, an example of the Department's public-private partnership efforts
- The partnership works with importers, carriers, brokers and other industry sectors emphasizing a seamless security conscious environment throughout the world-wide commercial supply chain

International Port Security Program (IPSP)

- A U.S. Coast Guard initiative to assess and evaluate vulnerabilities and antiterrorism measures taken in foreign ports

H.R. 2886, Department of Homeland Security Financial Accountability Act is ordered reported favorably out of the Homeland Security Committee.

(Back row L-R) Vice Chairwoman Jennifer Dunn (WA), Chairman Cox, and Ranking Member Turner; (In Front) Congressman Robert Andrews (NJ) at Full Committee Hearing held on Progress in Addressing Management Challenges at the Department of Homeland Security

- A Washington, DC-based team will use internationally negotiated treaties and standards as the baseline for assessing the effectiveness of port and foreign vessel security measures implemented by foreign countries and Flag Administrations
- As part of IPSP, International Port Security Liaison Officers will be assigned to strategic locations throughout the world to monitor the port security situation on a continuous basis

The Department is taking numerous actions to protect America's ports and coasts – 95,000 miles of maritime border – against terrorist attack. New legislation and international standards have fundamentally changed the security culture of the entire maritime community. More has been done to secure our ports since September 11, 2001 than at any time since World War 2.

On July 1, 2004, regulations came into effect requiring all U.S. ports, maritime facilities, and vessels calling on U.S. ports to conduct vulnerability assessments and implement security plans. The **U.S. Coast Guard** has partnered with the maritime industry, state and local governments, the international community, and private citizens to ensure that U.S. ports and waterways continue to run efficiently and effectively while the new security regime is put in place. In the first month of enforcement, the Coast Guard inspected over 200 domestic vessels, 250 port facilities, and restricted the operations of 30 vessels and 20 port facilities for failure to comply with the new regulations. The Coast Guard also successfully employed its Port State Control program, inspecting all foreign vessels upon first arrival to the U.S. and has controlled or denied entry to over 80 foreign vessel for failure to comply with international security standards.

H.R. 3266, The Faster and Smarter Funding for First Responders Act of 2003 passes unanimously in the House Homeland Security's Subcommittee on Emergency Preparedness and Response.

The Coast Guard has grown by over 4,100 personnel since the terrorist attacks and has received a budget increase for homeland security related activities of over 60%. During this time, the Coast Guard conducted more than 124,000 port security patrols, 13,000 air patrols, boarded more than 92,000 vessels, interdicted over 14,000 individuals attempting to enter the United States illegally, and created and maintained more than 90 Maritime Security Zones.

Federal investment in port security is also up from under $200 million in fiscal year 2001 to over $2.3 billion in fiscal year 2005. The federal port security grant program, developed after September 11th, has awarded over $500 million to over 1,000 domestic port projects to help improve security. While this is a marked improvement from pre-September 11th days, the Committee remains steadfast in its oversight of the Department's port security capabilities.

Another DHS maritime security initiative is the Coast Guard **Maritime Safety and Security Teams (MSSTs)**

- Units are specifically dedicated to the port security mission
- These 75 member teams are assigned to the nation's critical seaports to enforce maritime law and provide counterterrorism protection
- Units are specially trained to protect and defend critical infrastructure, enforce security zones, and to react and respond to terrorist incidents

Chairman Cox (second from left) and Members of the Committee meet with Israeli Prime Minister Ariel Sharon

Committee Delegation tours Spain, Italy, Syria, Israel, and Turkey to exchange views and encourage cooperation in the war on terrorism. The Delegation meets foreign officials including Ignacio Astarloa, State Secretary for Security in Spain; Giuseppe Pisanu, Minister of the Interior in Italy; Bashar al-Asad, President of Syria; and Ariel Sharon, Prime Minister of Israel.

- Currently, there are 13 MSSTs based in commercial and strategic ports throughout the United States, including New York, Seattle, Los Angeles/Long Beach, and Boston
- Since their inception Coast Guard MSSTs have protected the Iraqi Freedom military load-outs, the Democratic National Convention, G-8 Summit, and the Olympics.

Path Forward

- DHS continues to improve upon its maritime security initiatives, extending America's security perimeter to overseas ports that ship cargo to the United States. To further progress in this area, DHS should focus on improving the coordination of the surveillance and interdiction functions among the air and marine assets of the Coast Guard, U.S. Immigration and Customs Enforcement (ICE), and U.S. Customs and Border Protection (CBP); developing a consolidated acquisition and maintenance program for air and marine assets that includes the modernization needs of each service; and integrating access to data and targeting information between agencies.
- Improved coordination and integration of the maritime security mission within DHS will help the Coast Guard, ICE, CBP mature into a cohesive organization that effectively enhances homeland security while reducing overlap and duplication of effort.
- All appropriate personnel of the Border and Transportation Security Directorate must have the capability to promptly access and receive law enforcement and intelligence information contained in all databases utilized by the Directorate. Additionally, there must be prompt transmittal of information between entities of the BTS Directorate and the IAIP Directorate for dissemination to other members of the intelligence community. The Committee believes that this is essential for the agencies within BTS to effectively and efficiently "connect the dots" by ensuring each agency has full and timely access to all information obtained by and available within the BTS Directorate.

Full Committee hearing is held on "The Homeland Security Advisory System: Improving Preparedness through Effective Warning." Admiral James Loy, Deputy Secretary of Homeland Security, and John O. Brennan, Director of the Terrorist Threat Integration Center, provide testimony.

- DHS should develop a plan to coordinate the targeting and screening systems within the National Targeting Center at CBP, the Law Enforcement Support Center at ICE, and the Transportation Security Administration's Transportation Security Operations Center. A key element of the coordination must include electronic linkage to all anti-terrorist related operations and watch centers within the Department, as well as the Terrorist Screening Center.

Protecting Critical Infrastructure

The Department

DHS is steadily introducing programs and implementing policies to protect our nation's critical infrastructure, both physical and virtual. Most notable will be completion of the National Infrastructure Protection Plan (NIPP). This plan, the first-ever comprehensive, risk-based security plan encompassing all of our nation's critical infrastructure sectors, is being developed in close collaboration with Sector Specific Agencies (SSAs) and the private industry.

"The development and initial operating capability of the National Cyber Alert System elevates awareness and helps improve America's IT [Information Technology] security posture. We are focused on making the threats and recommended actions easier for all computer users to understand, prioritize, and act upon. We recognize the importance and urgency of our mission and are taking action"

(Amit Yoran, director of the National Cyber Security Division, Department of Homeland Security, January 28, 2004)

★★ February 27-29, 2004 ★★

Committee Delegation tours U.S. Southern Command in Florida; the Coast Guard Operations Center in the U.S. Virgin Islands; and the U.S. Naval Base at Guantánamo Bay, Republic of Cuba.

National Infrastructure Protection Plan (NIPP)

- Provides a risk-based framework for the implementation of the Homeland Security Act and Homeland Security Presidential Directive-7 ("Critical Infrastructure Identification, Prioritization, and Protection") mandates
- Has provided structure for the coordination of Sector Specific Agency Sector Security Plans (SSPs) with the overall national effort to enhance critical infrastructure protection
- DHS has developed and issued guidance and templates for SSA Security Plans
- The SSPs and the NIPP include measures to assess security program effectiveness
- As of July of 2004, SSPs have been completed and reviewed for compliance and content by DHS
- DHS is in the process of integrating the SSPs with a National Level Integration Plan
- The comprehensive National Infrastructure Protection Plan will be completed in October 2004
- The Committee must provide strong oversight to make certain NIPP is completed and implemented.

Information Analysis and Infrastructure Protection Directorate (IAIP)

- Has worked aggressively with the private sector and state and local governments to define roles and responsibilities among critical infrastructure sectors. This is a work in progress that will require close and sustained Congressional oversight.
- Established the Homeland Security Operations Center (HSOC), a 24 hours a day, 7 days a week (24/7) operation that collects and fuses law enforcement and intelligence community information, acts as the primary national hub for operational communications and information sharing in the event of a domestic terrorist incident, and acts as the primary conduit for domestic situational awareness for the White House Situation Room
- Developed, published, and distributed to the chemical sector and law enforcement authorities *Report of Common*

The Faster and Smarter Funding for First Responders Act of 2003 is ordered reported record vote of 37 yeas and 0 nays out of the Homeland Security Committee.

Vulnerabilities to Terrorism at Chemical Facilities, Potential Indicators of Terrorist Activity: Chemical Facilities and Community-Based Security Buffer Zone Plans

Office of Infrastructure Protection (IP) is DHS's primary conduit for protecting America's critical infrastructure and key assets and is aggressively moving forward through a variety of operational strategies. IP is comprised of three divisions as well as numerous teams and programs:

Protective Security Advisory Teams (PSAT)

- 20 teams of 8 advisors each visit sites of highest risk to provide training and support, and to assist site personnel and local law enforcement in developing protection plans
- DHS is developing a common vulnerability assessment methodology and a common protection methodology for critical infrastructure components

Protective Security Advisor Program (PSAP)

- Beginning in August 2004, will provide a field-deployed liaison hub for local, state and federal entities, and the private sector with DHS

Chairman Christopher Cox, Tom DeLay, TX, House Majority Leader, and Chairman John Shadegg, AZ, Subcommittee on Emergency Preparedness and Response (left to right)

- 68 Protective Security Advisors will be posted across the nation in a risk-based strategic alignment with critical infrastructure densities
- PSAs will greatly enhance critical infrastructure identification, vulnerability assessment, and implementation of protection programs, significantly improving the security posture of our nation's critical infrastructure

Protective Security Division (PSD) focuses on developing community-based critical infrastructure planning and prevention

Full Committee hearing held, "Towards a National Biodefense Strategy," with Penrose "Parney" Albright, Assistant Secretary of Homeland Security for Science and Technology, among witnesses.

strategies with a focus on public-private partnership

Infrastructure Coordination Division (ICD)

- Manages private industry interactions, facilitating the sharing of infrastructure related information, including threats and vulnerabilities, incidents and events, potential protective measures and best practices.
- To secure the virtual infrastructure, the U.S. Computer Emergency Response Team (US-CERT) is working with infrastructure owners and operators and technology experts to foster the development of improved security technologies and methods to drive increased cyber security at all levels across the nation – from citizens in their homes and at work, to private sector companies, government agencies and organizations.

National Cyber Security Division (NCSD)

- Provides for 24/7 functions to protect America's virtual infrastructure, including conducting cyberspace analysis, issuing alerts and warning, improving information sharing, responding to major incidents, and aiding in national-level recovery efforts.
- Managed by US-CERT and NCSD, the newly-created National Cyber Alert System is America's first coordinated national cyber security system for identifying, analyzing, and prioritizing emerging vulnerabilities and threats. It provides the first infrastructure for relaying graded computer security update and warning information to all users.

DHS integrated the **National Communications System (NCS)** to facilitate reliable communications between our nation's most vital government and private industry centers in the case of terrorist attack.

Path Forward

- DHS and IP in particular should, in coordination with private industry and State Homeland Security Advisors, continue to develop a more collaborative relationship with state and local law enforcement officials in order to build greater consistency in the identification of critical infrastructure and the implementation of protective measures.
- DHS should increase its focus on addressing the vulnerabilities existent in the realms of interdependence between the various

Subcommittee on Infrastructure and Border Security hearing held on "Protecting the Homeland: Building a Layered and Coordinated Approach to Border Security," with David V. Aguilar, Chief of the U.S. Border Patrol among witnesses.

Secretary of Homeland Security Tom Ridge (Center) testifying at Full Committee Hearing held on the Department of Homeland Security's Proposed Fiscal Year 2005 Budget.

critical infrastructure sectors. With SSAs focusing on their respective sectors, DHS must fill this void.

- In areas where collaboration with SSAs is unclear, ineffective or inefficient, DHS must more consistently consult with Congress – and specifically the Committee on Homeland Security – to find solutions.
- DHS should develop and publish a strategy for effective cooperation in the identification and protection of critical infrastructure with all SSAs and, where necessary, specific strategies for individual SSAs.
- DHS should have a coordinated, focused cyber security program as outlined in HR 5068 (Cyber Security Enhancement Act) introduced by Mr. Thornberry and Ms. Lofgrin, creating an Assistant Secretary for cyber security.

Full Committee met to consider Department of Homeland Security Authorization for Fiscal Year 2005, but did not complete consideration thereon.

Applying New Technologies

Innovation, collaboration, and rapid technology delivery have been the mission priorities of the Department of Homeland Security's Science and Technology Directorate (S&T). The Department quickly developed coordinated research initiatives across the public and private sector scientific communities to make progress on the highest priority issues such as biological, chemical, radiological and nuclear detection and countermeasures; risk assessment and communication; and rapid response capabilities. Key to the Directorate's continued success will be working with the first responder community to identify needs and provide solutions, while balancing short-term product delivery with long-term research investments.

Chairman Thomas H. Kean (L) and Vice Chairman Lee H. Hamilton (R) of the National Commission on Terrorist Attacks Upon the United States testifying at Full Committee Hearing on Homeland Security: The 9/11 Commission and the Course Ahead

The Department

Leveraging our national scientific assets to protect our citizens and critical infrastructure from a terrorist incident is a key mission priority for the S&T Directorate.

One of the immediate challenges that the S&T Directorate had to solve was the ability to quickly detect a chemical, biological, radiological and nuclear (CBRN) incident. In response to this challenge the Department implemented the **Biowatch** program to numerous high risk cities across the nation. The program uses environmental sampling devices to quickly detect biological agents, such as anthrax, so that countermeasures can be administered to affected citizens.

On January 29, 2004, the Homeland Security and Health and Human Services Secretaries announced a $274 million **Bio-Surveillance Program** that improves on-going CBRN surveillance programs. These surveillance and detection programs will be further supported

Full Committee held, "9/11 Commission: Toward a Paradigm for Homeland Security Information Sharing," with Thomas H. Kean, Chairman, and Lee H. Hamilton, Vice Chairman, both of the National Commission on Terrorist Attacks Upon the United States, among witnesses.

and enhanced by the **National Biodefense Analysis Countermeasures Center (NBACC)** established at Fort Detrick by the S&T Directorate.

The S&T Directorate and the Washington Metropolitan Area Transit Authority (WMATA), recently completed **PROTECT (Program for Response Options and Technology Enhancements for Chemical/ Biological Terrorism)**, which is an operational chemical agent detection and response program, deployed in more than six subway stations. Upon completion, this program will be expanded to other facilities across the nation.

The S&T Directorate and its partners at the San Francisco International Airport are working on a pilot program that couples biological and chemical detection with vulnerability analysis, response, and restoration. This program integrates networking sensors with the operation of ventilation systems, enabling systems to redirect contaminated air, to improve evacuation in the event of an emergency.

The S&T Directorate has also made protecting our ports and land borders a priority. It now directly manages the Port Authority of New York and New Jersey's radiation detection test bed. DHS broadened the project beyond testing and evaluation of individual pieces of technology to a systems approach including response protocols and operational concepts to safe guard our ports from a radiological or nuclear device.

The S&T Directorate also initiated the **Border Safety Integrated Feasibility Experiment.** This program creates an infrastructure in the Southwest U.S. for data sharing between the Department's Border and Transportation Security Directorate and local and state law enforcement officials.

Under Secretary for Science and Technology Charles McQueary (L) answers question from Chairman Cox (R) at Subcommittee on Cybersecurity, Science and Research & Development Hearing held on Homeland Security Science and Technology Budget for Fiscal Year 2005.

Full Committee hearing held on "Homeland Security: The 9/11 Commission and the Course Ahead." Tom Ridge, Secretary of Homeland Security, gives testimony.

To protect our passenger aircrafts the S&T Directorate established the **Counter-MANPADS Program** to address the potential threat that Man-Portable Air Defense Systems (MANPADS) pose to commercial aircraft. The Counter-MANPADS Program Office is working to take advantage of existing military research and commercial technologies to protect our passenger planes from shoulder fired missiles.

The private sectors have or will develop technologies to make our borders, seaports, airports, and other infrastructure safer. The public and private sectors join most directly where basic research meets applied technology. Since its establishment, the S&T Directorate through its **Homeland Security Advanced Research Projects Agency (HSARPA)** has completed two major solicitations on radiological and nuclear detection and architecture and is working on six other proposals.

DHS is reaching out to small business innovators as well:

- Over 60 firms received a total of $6.5 million, with individual firms each receiving up to $100,000 for a period of six-months to develop new technologies.
- This year DHS issued designations and certifications for four anti-terrorism technologies under the **SAFTEY Act (Support Anti-terrorism by Fostering Effective Technologies Act of 2002).**
- The SAFETY Act is designed to encourage the development and rapid deployment of anti-terrorism technologies by providing manufacturers and sellers with limited liability risks.

To assist IAIP's National Cyber Security Division, the Science and Technology division created a **Cybersecurity Research & Development Center** which has already started making advances in such areas as honeynets to capture and analyze malicious code, Internet mapping and simulation, protocol analysis, and securing process control systems. Their research and applied development projects are vital for providing funding and direction to help secure the cyber elements of our nation's critical infrastructure.

Path Forward

A direct result of this vigorous oversight was authorization legislation that addresses several cross-cutting issues relating to technical integration, organizational improvement, technology transfer, and long term investment in Research and Development as well as establishing performance measures for the Directorate. Specifically, the Committee recommends:

- Establishing a technology transfer program to get equipment, products and services

deployed faster to users on the homeland security front lines.

- Creating a communications interoperability program for state, local and federal first responder partners.
- Tasking DHS to develop a national biodefense and radiological and nuclear threat mitigation strategy that includes threat and risk analysis across different parts of the federal government.
- Creating a geospatial office within the Department.
- Providing an additional $40 million for University Programs for a total of $70 million investment to advance homeland security science.

Preparing for Response

The September 11th attacks created a new mission for our nation's first responders – preparing for and responding to acts of terrorism. The President and Congress reacted swiftly, creating agencies within DHS to prepare for and respond to terrorist attacks and increasing terrorism preparedness funding for first responders.

The Department

The **Emergency Preparedness and Response Directorate (EP&R)** was largely established by the transfer of the **Federal Emergency Management Agency (FEMA)** into DHS. The directorate helps ensure the effectiveness of emergency response providers, provides the federal government's response to terrorist

attacks and major disasters, and aids in subsequent recovery from any such incident.

The **Office of State and Local Government Coordination and Preparedness (OSLGCP)**, located within the Office of the Secretary, has the specific responsibility for the preparedness of the United States for acts of terrorism, which it accomplishes through grant distribution, training programs, and exercises. In addition to streamlining the application process, DHS also requires every state to conduct and submit a thorough needs assessment, known as a **State Homeland Security Strategy**, to ensure the proper, strategic use of grant funds.

Through EP&R and OSLGCP, therefore, DHS maintains a federal response capability while also preparing first responders at the state and local level.

First responders face new challenges, beyond the scope of their traditional missions, in managing large and complex responses to acts of terrorism. In New York City, for instance, the 9/11 Commission reported problems with incident command, coordination, and interoperability. DHS has worked diligently to address these new challenges and the problems they pose.

First, to define how disparate responders would best coordinate their on-scene activities, DHS developed and released the **National Response Plan** and the **National Incident Management System (NIMS)**.

- National Response Plan defines the respective roles of federal departments in responding to any emergency or disaster.
- NIMS establishes an on-the-ground, nationwide approach to facilitate the on-scene interactions of first responders from any level of government or the private sector

DHS also established a **National Exercise Program** to test the coordination and response capabilities of federal, state, local, tribal and foreign entities. In coordination with DHS, state and local governments hold frequent exercises to sharpen local responses. At the national level, DHS has coordinated the **Top Officials (TOPOFF)** exercises to test the joint responses of federal, state, and local authorities to a weapons-of-mass-destruction attack. DHS has conducted two TOPOFF exercises, with the third scheduled for 2005.

In addition, DHS has focused its efforts to enhance interoperable communications through **Project SAFECOM**:

- Serves as the umbrella program within the federal government to coordinate interoperability issues among a diverse group of stakeholders
- This year, Project SAFECOM released the first ever Statement of Requirements for interoperability, which is the initial step in rigorously defining the functional needs of first responders.
- In addition, DHS will soon announce the completion of short-term patching solutions to enable fully interoperable communications in select high-risk cities.

The Committee

Notwithstanding this significant progress, the Committee found that DHS distributed billions of dollars in terrorism preparedness grants without regard to risk or capabilities. Rather, DHS distributed these important funds based on arbitrary, political formulas. In response, the Committee held numerous hearings to better understand the grant distribution process and how best to reform it. Based on these hearings and other rigorous investigation, the Committee issued a report in April 2004 assessing both the timeliness and effectiveness of the distribution process. Entitled **"An Analysis of First Responder Grant Funding,"** the report identified common causes for delayed spending, assessed the degree to which federal and state governments accounted for risk in distributing grant funds, and highlighted many examples of questionable grant spending.

To reform the grant-making process, the Committee introduced **H.R. 3266, The Faster and Smarter Funding for First Responders Act**, in October 2003. H.R. 3266 emphasizes the need to distribute grant funding on the basis of risk and to define minimum essential capabilities of preparedness for different types

of communities. Over 24 first responder organizations, including the largest law enforcement and fire service groups, have endorsed the bill. On April 2, 2004, the Committee reported out H.R. 3266; the other four Committees of referral followed suit. H.R. 3266 awaits action by the full House.

Path Forward

- As DHS continues to distribute billions of dollars in first responder grants, the Committee strongly believes that risk must be the primary factor in allocating grants at both the federal and state levels. Other imperatives should include the development of specific, flexible, measurable, and comprehensive preparedness goals and the creation of a faster distribution process.

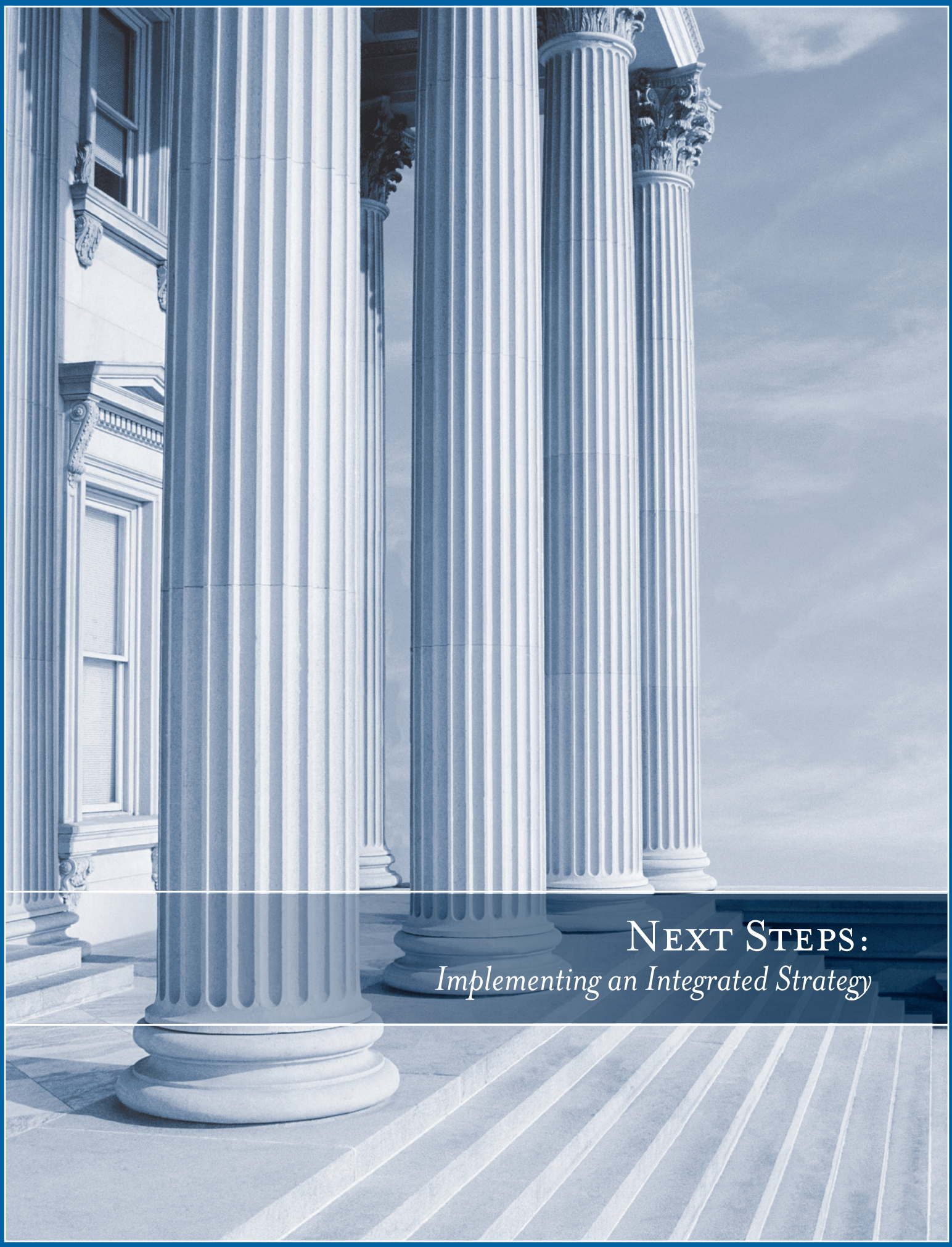
- To implement risk-based funding, DHS must enhance its capability to assess accurately risks throughout the nation. Specifically, DHS needs to integrate information about vulnerabilities from local sources, which are most knowledgeable about their jurisdictions, with threat information provided by intelligence and law enforcement groups.
  Such integration would enable DHS to develop a more refined picture of the risks faced by different communities and, thus, allocate scarce resources more effectively.

Chairman Cox (L) standing with Ranking Member Turner (R)

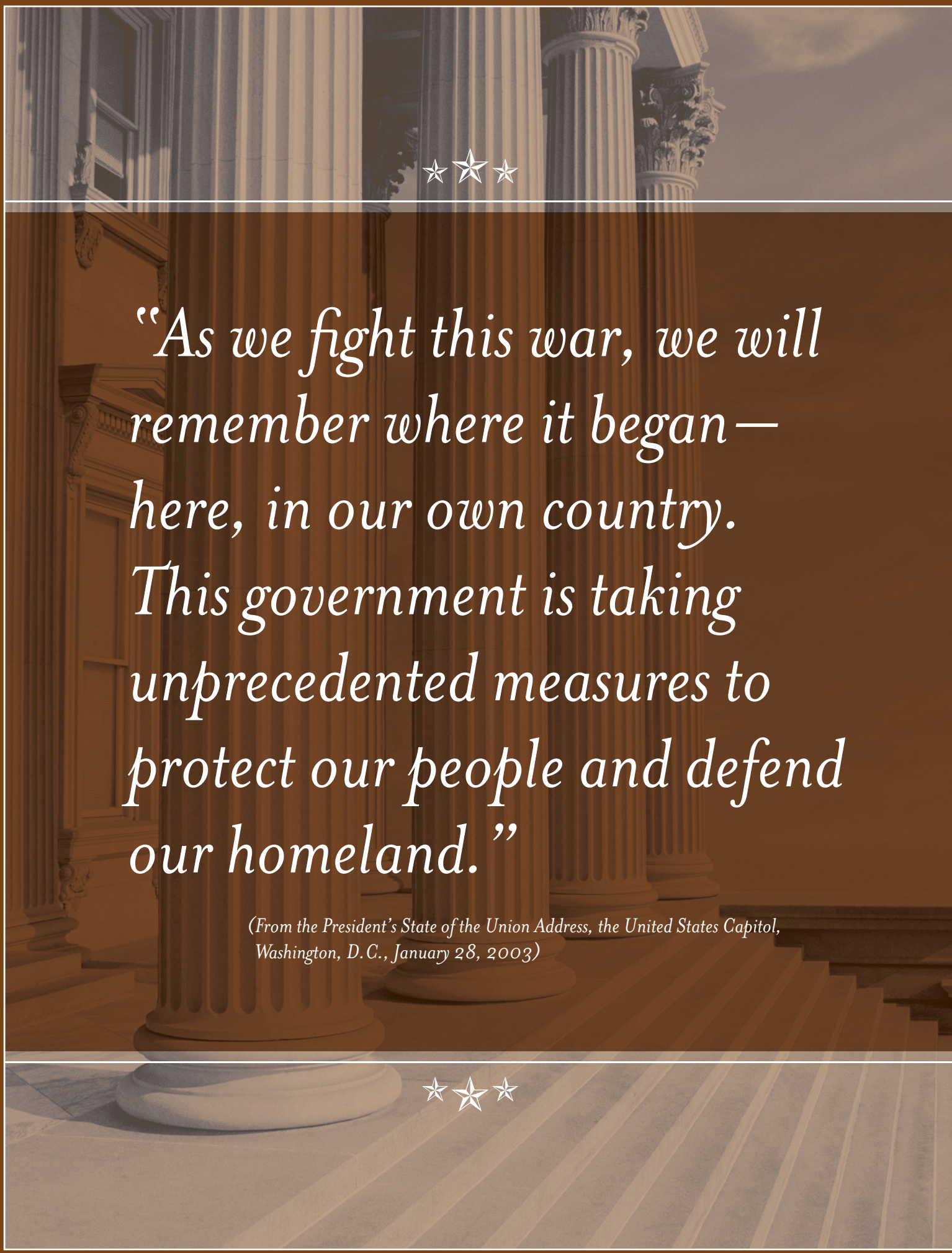
- The Committee believes that NIMS should be fully implemented across the first responder community, including medical health professionals, to ensure better on-scene incident management.

- The Committee also believes that DHS exercise and training programs should be prioritized and integrated across the federal, state, and local levels.

- Finally, the Committee recognizes the importance of interoperable communications and the difficulty of achieving this goal. Project SAFECOM must be given real authority to carry out its mandate; in the interim, short-term patching solutions must be prioritized for high-risk areas.



Next Steps:
Implementing an Integrated Strategy



"As we fight this war, we will remember where it began—here, in our own country. This government is taking unprecedented measures to protect our people and defend our homeland."

(From the President's State of the Union Address, the United States Capitol, Washington, D.C., January 28, 2003)

The September 11th attacks changed America as it changed the world. The Bush Administration took comprehensive and decisive action to prevent another terrorist attack on the U.S. homeland. In this, the Administration succeeded.

Yet now we must move from defensive reaction to smart strategy to defeat our terrorist enemies.

An integrated homeland security strategy takes into account these priorities:

- **Further Integration:** The Department, while respecting the traditional missions of legacy agencies, must move more steadily toward integrated management, procurement, information technology, and human resource systems to create a common culture committed to countering the terrorist threat.
- **Improved Intelligence:** The central component of the Department's counterterrorism mission is intelligence. It must, therefore, build the analytic capabilities, especially against the bio and cyber threats, to perform anticipatory defensive measures. DHS needs to show greater progress, in particular, against the top priority cyber threat
- **Public-Private Partnership:** The Department must work with the private sector, which controls over eighty-five percent of the nation's critical infrastructure, to ensure that steady progress is made in sharing actionable information on the terrorist threat. We have much more work to do in this area. In addition, identifiable vulnerabilities need to be prioritized and addressed to make the country safer.
- **Permanent Oversight:** A permanent Department of Homeland Security will require a consolidation of Congressional oversight to guide the Department effectively and to relieve it of uncoordinated demands from multiple committees and subcommittees. As recommended by the 9/11 Commission, the Committee will work with the Congress to create a permanent Homeland Security Committee.

Measuring Progress Toward a Safer America

The primary goal for Fiscal Year 2005 is for DHS and the Congress to establish performance metrics on the implementation of a clear strategy for homeland security.

The strategy must focus resources and dollars on agreed-upon priorities to make the country safer. The nation needs a clearer understanding of what homeland security is and what it will cost the American people in the years ahead. We must get DHS right because it—like the threat of terrorism—is here to stay.

Next Steps

The Select Committee, in addition to its schedule of DHS-related hearings, will hold public hearings and extensive consultations with House leadership to develop, before the end of the 108th Congress, a proposal to amend Rule 10 to make our committee permanent and to assign it jurisdiction consistent with its responsibilities to conduct oversight over the Department as it implements the provisions of the Homeland Security Act.

The new Standing Committee will exercise focused and rigorous oversight over DHS —in collaboration with other committees of jurisdiction—as it implements the Homeland Security Act. Key elements in the committee's oversight will be:

- DHS organization and administration.
- The homeland security mission to prevent, prepare for, and respond to acts of terrorism.
- DHS capabilities to analyze infrastructure vulnerability and threat, to combine them in risk assessment, and to develop and implement security enhancements.
- DHS statutory responsibilities to communicate and collaborate with state, local, and corporate entities on threat and remediation.
- DHS statutory responsibilities to manage research and development programs, and to develop threat countermeasures and apply new technological applications to homeland security problems.
- DHS statutory responsibilities for the security of U.S. air, land, and maritime borders, ports of entry, and transportation systems against acts of terrorism to the homeland.

Only by moving from unfocused reaction to cost-effective strategy can we make America safer for the long term. Our defense of freedom today preserves it for future generations.

Special Thanks to:

John Gannon

Donovan Chau

The Select Committee on Homeland Security
U.S. House of Representatives, Washington D.C. 20515

Phone: (202) 226-8417 • Fax: (202) 226-3399 • email:homeland@mail.house.gov